IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

SOFIYA ANISIMOVA, individually and on behalf of all others similarly situated, Plaintiff, v. VILLAGE PRACTICE MANAGEMENT COMPANY, LLC d/b/a CITYMD, Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Sofiya Anisimova ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself, which are based on personal knowledge.

NATURE OF ACTION

1. Plaintiff brings this suit on behalf of all LinkedIn users who live in the United States and who scheduled an urgent care medical appointment through the website www.citymd.com (the "Website"). The Website is owned and operated by Defendant Village Practice Management Company, LLC d/b/a CityMD ("Defendant" or "CityMD").

2. Patients trust healthcare providers to safeguard their information. When booking medical appointments online, patients reasonably expect the sensitive and legally protected information related to their appointment will remain confidential and protected from third parties. Such an expectation is based, in part, on legal protections afforded to such information. Being able to trust that their health information is secure is essential to upholding patient rights and the integrity of our healthcare system.

3. Health information is incredibly valuable to online advertising companies. Despite the legal protections afforded to this sensitive information, advertising companies go to great lengths to intercept such information for use in their targeted advertising campaigns.

4. Unbeknownst to Plaintiff and members of the putative class, Defendant assisted LinkedIn Corporation ("LinkedIn") in intercepting sensitive and confidential communications, including the location and time of their medical appointments, their gender, and the type of medical appointments they were seeking treatment for (*see* Figures 2–5). Defendant never disclosed that it was sharing data related to its patients' medical appointments with third parties. Nor did Plaintiff or members of the putative class consent to such.

5. LinkedIn develops, owns, and operates "the world's largest professional network with more than 1 billion members in more than 200 countries and territories worldwide."[1] LinkedIn is also an advertising company that touts its ability to deliver targeted marketing to specific users.

6. Defendant assisted LinkedIn in intercepting this confidential information for target advertising purposes. Plaintiff brings this action for legal and equitable remedies resulting from these illegal acts.

THE PARTIES

7. Plaintiff is domiciled in Brooklyn, New York. Plaintiff maintained an active LinkedIn account at all relevant times when booking a medical appointment on the Website.

8. In or around March 23, 2024, Plaintiff scheduled a medical appointment through the Website. When booking her appointment, Plaintiff selected a CityMD location, a time, who she was booking an appointment for, her gender, and why she was booking the appointment.

[1] LINKEDIN, ABOUT, https://about.linkedin.com/?trk=homepage-basic_directory_aboutUrl.

Unbeknownst to Plaintiff, Defendant assisted LinkedIn in tracking her private activity on the Website using the LinkedIn Insight Tag. Defendant installed this software on its Website to assist LinkedIn in tracking Plaintiff and intercepting her communications with Defendant, including communications that contained confidential, health-related information concerning her medical appointment. Neither Defendant nor LinkedIn received consent from Plaintiff to track or sell her confidential and protected health data to advertisers. Defendant's acts and practices, as described herein, are an egregious breach of Plaintiff's privacy and a breach of its duty of confidentiality as a medical provider.

9. Defendant Village Practice Management Company, LLC d/b/a CityMD is a Delaware corporation with its principal place of business in Berkeley Heights, New Jersey. Defendant develops, owns, and operates the Website, which is used by patients throughout the United States, including New York, to book medical appointments.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the Electronic Communications Privacy Act, 18 U.S.C. § 2511). This Court also has supplemental jurisdiction over Plaintiff's state law claim under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiff alleges that at least 100 people comprise the proposed class, that the combined claims of the proposed class members exceed $5,000,000 exclusive of interest and costs, and that at least one member of the proposed class is a citizen of a state different from at least one defendant.

11. This Court has personal jurisdiction over Defendant because Defendant conducts substantial business within this District and a substantial part of the events giving rise to this claim occurred in this District.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to this claim occurred in this District.

FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS

A. The Health Insurance Portability and Accountability Act ("HIPAA")

13. Under HIPAA, a healthcare provider may not disclose personally identifiable information ("PII") or protected health information ("PHI") without the patient's express written authorization.[2]

14. The United States Department of Health and Human Services ("HHS") has established a national standard, known as the HIPAA Privacy Rule, to explain the duties healthcare providers owe to their patients. "The Rule requires appropriate safeguards to protect the privacy of [PHI] and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization."[3]

15. A healthcare provider violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-d9 ("Part C"): "(1) uses of causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."[4]

16. The statute states that an entity "shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity…and the individual obtained or disclosed such information without authorization." *Id.*

---

[2] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

[3] U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

[4] 42 U.S.C. § 1320d-6.

17. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to its patients.

18. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained and transmitted in violation of 45 C.F.R. Section 164.306(a)(1);

(b) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.R.F. Section 164.308(a)(1);

(c) Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation of 45 C.F.R. Section 164.308(a)(6)(ii);

(d) Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. Section 306(a)(2);

(e) Failing to protect against reasonably anticipated uses of disclosures of electronic PHI not permitted under privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. Section 164.306(a)(3); and

(f) Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. Section 164.530(c).

19. Health care organizations regulated under HIPAA, like Defendant, may use third-party tracking tools, such as the LinkedIn Insight Tag, *in a limited way* to perform analysis on data key to operations.

20. They are not permitted, however, to use these tools in a way that may expose patients' PHI to third-party vendors. As explained by the HHS:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. **For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures**.[5]

21. The Bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, **because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.**[6]

22. Plaintiff and Class members face the exact risks for which the government expresses concern. Defendant's unlawful conduct resulted in third parties intercepting information regarding Plaintiff and Class members medical appointment scheduling on Defendant's Website.

---

[5] HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES (THE "BULLETIN") (EMPHASIS ADDED), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[6] *Id.* (emphasis added).

23. The Bulletin further makes clear how broad the government's view of protected information is:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, **or any unique identifying code**.[7]

24. The Bulletin goes even further:

> All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[8]

25. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning regulated entities about the privacy and security risks arising from the use of online tracking technologies:

> The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers [regulated entities] about the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.
>
> "When consumers visit a hospital's [regulated entity's] website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."

---

[7] *Id.* (emphasis added).

[8] *Id.* (emphasis added).

> "Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital's [regulated entity's] website," said Melanie Fontes Rainer, OCR Director. "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."
>
> The two agencies sent the joint letter to approximately 130 [regulated entities] hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.
>
> In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, ***medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment***.[9]

26. Accordingly, Defendant's conduct, as described more thoroughly below, is in violation of federal law and the clear pronouncements by the FTC and HHS.

B. LinkedIn's Platform and Business Tools

27. LinkedIn markets itself as "the world's largest professional network on the internet[.]"[10] But LinkedIn is no longer simply a tool to help users find jobs or expand their professional network. LinkedIn has moved into the marketing and advertising space and boasts of its ability to allow potential advertisers to "[r]each 1 billion+ professionals around the world" via

[9] Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking (emphasis added).

[10] LINKEDIN, WHAT IS LINKEDIN AND HOW CAN I USE IT?, https://www.linkedin.com/help/linkedin/answer/a548441#.

its Marketing Solutions services.[11] Recently, LinkedIn was projected as being responsible for "roughly 0.9 percent of the global ad revenue" which included approximately $5.91 billion in advertising revenue in 2022.[12]

28. According to LinkedIn, "[t]argeting is a foundational element of running a successful advertising campaign — [g]etting your targeting right leads to higher engagement, and ultimately, higher conversion rates." [13] Targeting refers to ensuring that advertisements are targeted to, and appear in front of, the target demographic for an advertisement. To that end, LinkedIn's Marketing Solutions services allow potential advertisers to "[b]uild strategic campaigns" targeting specific users.[14] LinkedIn's "marketing solutions allow advertisers to select specific characteristics to help them reach their ideal audience. The ads [users] see on LinkedIn are then targeted to provide content relevant to [the users]."[15]

29. As a result of its activities and operation of the LinkedIn Insight Tag, LinkedIn is able to make extremely personal inferences about individuals' demographics, intent, behavior, engagement, interests, buying decisions, and more.[16]

---

[11] LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions.

[12] Valentina Dencheva, *LinkedIn annual ad revenue 2017-2027*, STATISTA (Dec. 12, 2023), https://www.statista.com/statistics/275933/linkedins-advertising-revenue.

[13] LINKEDIN, REACH YOUR AUDIENCE: TARGETING ON LINKEDIN, p.3, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/resources/pdfs/linkedin-targeting-playbook-v3.pdf.

[14] LINKEDIN, *supra* note 11.

[15] LINKEDIN, LINKEDIN ADS AND MARKETING SOLUTIONS, https://www.linkedin.com/help/lms/answer/a421454.

[16] *See* LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions/audience ("Target audiences through demographic marketing[,]" "Zero in on intent, behavior, engagement, interests, and more[,]" and "Reach the LinkedIn audience involved in the buying decision").

30. The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network.[17]

31. Such information is extremely valuable to marketers and advertisers because the inferences derived from users' personal information and communications allows marketers and advertisers, including healthcare providers and insurance companies, to target potential customers.[18]

32. For example, through the use of LinkedIn's Audience Network, marketers and advertisers are able to expand their reach and advertise on sites other than LinkedIn to "reach millions of professionals across multiple touchpoints."[19] According to Broc Munro of Microsoft, "[w]e gravitate towards social platforms like LinkedIn to achieve more targeted marketing engagement. However, we know that our audiences don't spend all their time on social media.

---

[17] *See id.*

[18] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy ("We serve you tailored ads both on and off our Services. We offer you choices regarding personalized ads, but you cannot opt-out of seeing other ads."); LINKEDIN, ACCOUNT TARGETING, https://business.linkedin.com/marketing-solutions/ad-targeting ("Target your ideal customer based on traits like their job title, company name or industry, and by professional or personal interests"); LINKEDIN, EXAMPLES OF TRENDING AND BEST-IN-CLASS HEALTHCARE CAMPAIGNS AND CONTENT, p.6, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/lkin-lms-sales-healthcare-campaigns-trending-content-Jan2023.pdf ("BD zeroed in on the end-benefit with a 30 second video introducing their PIVO needle-free blood collection device to potential customers."); LINKEDIN, HEALTHCARE SOCIAL MEDIA STRATEGIES FOR 2023, p.1, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/hc-social-media-trends.pdf (listing "potential customers" as "Common audiences" for insurance sector).

[19] LINKEDIN, ACCOUNT TARGETING, https://business.linkedin.com/marketing-solutions/ad-targeting.

LinkedIn Audience Network enables us to expand our reach to trusted sites while still respecting our audience targeting. This increases the impact of our advertising."[20]

33. In July 2022, "LinkedIn Marketing Solutions surpassed $5 billion in annual revenue[.]"[21] That figure is "expected to further grow to reach 10.35 billion U.S. dollars by 2027."[22]

34. According to LinkedIn, the LinkedIn Insight Tag is "[a] simple code snippet added to [a] website [that] can help you optimize your campaigns, retarget your website visitors, and learn more about your audiences."[23] LinkedIn represents that the LinkedIn Insight Tag "enable[s] in-depth campaign reporting and unlock[s] valuable insights about your website visitors."[24]

35. LinkedIn's current iteration of its Insight Tag is a JavaScript-based code which allows for the installation of its software.[25] A critical feature allows the LinkedIn Insight Tag to track users, even when third-party cookies are blocked.[26] LinkedIn "recommend[s] using the JavaScript-based Insight Tag or Conversions API" because third-party cookie settings are being

---

[20] LINKEDIN, LINKEDIN AUDIENCE NETWORK, https://business.linkedin.com/marketing-solutions/native-advertising/linkedin-audience-network.

[21] *LinkedIn Business Highlights from Microsoft's FY22 Q4 Earnings*, LINKEDIN PRESSROOM (July 25, 2022), https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time.

[22] Dencheva, *supra* note 12.

[23] LINKEDIN, INSIGHT TAG, https://business.linkedin.com/marketing-solutions/insight-tag.

[24] LINKEDIN, LINKEDIN INSIGHT TAG FAQS, https://www.linkedin.com/help/lms/answer/a427660.

[25] LINKEDIN, *supra* note 23.

[26] *Id.* ("It's important for advertisers to prepare for these changes by switching to JavaScript tags and enabling 'enhanced conversion tracking' in the Insight Tag settings to continue capturing signals where 3rd party cookies are blocked.").

deprecated across the industry.[27] Embedding the JavaScript as a first-party cookie causes users' browsers to treat the LinkedIn Insight Tag as though it is offered by the website being visited, rather than by LinkedIn. Doing so ensures that the third-party cookie-blocking functions of modern web browsers do not prevent LinkedIn from collecting data through its software.[28] Instead, the LinkedIn Insight Tag is shielded with the same privacy exemptions offered to first-party cookies.

36. When a user who has signed in to LinkedIn (even if the user subsequently logs out) is browsing a website where the LinkedIn Insight Tag has been embedded, an HTTP request is sent using cookies, which includes information about the user's actions on the website.

37. These cookies also include data that differentiate users from one another and can be used to link the data collected to the user's LinkedIn profile.

38. The HTTP request about an individual who has previously signed into LinkedIn includes requests from the "li_sugr" and "lms_ads" cookies. Each of these cookies are used by LinkedIn "to identify LinkedIn Members off LinkedIn" for advertising purposes.[29]

39. For example, the "li_sugr" cookie is "[u]sed to make a probabilistic match of a user's identity."[30] Similarly, the "lms_ads" cookie is "[u]sed to identify LinkedIn Members off LinkedIn for advertising."[31]

40. A LinkedIn profile contains information including an individual's first and last name, place of work, contact information, and other personal details. Based on information it

---

[27] *See id.*

[28] *See id.*

[29] LINKEDIN, LINKEDIN COOKIE TABLE, https://www.linkedin.com/legal/l/cookie-table.

[30] *See id.*

[31] *See id.*

obtains through the LinkedIn Insight Tag, Defendant LinkedIn is able to target its account holders for advertising.

41. LinkedIn never receives consent from users to intercept and collect electronic communications containing their sensitive and unlawfully disclosed information. In fact, LinkedIn expressly warrants the opposite.

42. When first signing up, a user agrees to the User Agreement.[32] By using or continuing to use LinkedIn's Services, users agree to two additional agreements: the Privacy Policy[33] and the Cookie Policy.[34]

43. LinkedIn's Privacy Policy begins by stating that "LinkedIn's mission is to connect the world's professionals . . . . Central to this mission is our commitment to be transparent about the data we collect about you, how it is used and with whom it is shared."[35]

44. The Privacy Policy goes on to describe what data LinkedIn collects from various sources, including cookies and similar technologies.[36] LinkedIn states "we use cookies and similar technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your device(s) on, off and across different services and devices where you have engaged with our Services. We also allow some others to use cookies as described in our Cookie Policy."[37]

---

[32] LINKEDIN, USER AGREEMENT, https://www.linkedin.com/legal/user-agreement.

[33] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy.

[34] LINKEDIN, COOKIE POLICY, https://www.linkedin.com/legal/cookie-policy.

[35] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy.

[36] *Id.*

[37] *Id.*

45. However, LinkedIn offers an express representation: "**We will only collect and process personal data about you where we have lawful bases.**"[38]

46. Despite this explicit representation, LinkedIn intentionally intercepts and receives sensitive and unlawfully disclosed information in violation of state and federal privacy laws.

47. Defendant assisted LinkedIn in these unlawful interceptions.

48. Users never choose to provide sensitive information to LinkedIn because, among other reasons, they never know whether a particular website uses the LinkedIn Insight Tag, and, if so, what sensitive personal data it collects.

49. At all relevant times, Defendant installed the LinkedIn Insight Tag on its Website for targeted advertising purposes.

C. How LinkedIn Intercepted Plaintiff's and Class Members' Protected Health Information

50. CityMD is a provider of accessible healthcare services that permits patients to schedule appointments at their brick-and-mortar locations through its Website. Upon entering the Website, CityMD warrants that it will help patients receive "care that can't wait."

51. To begin, patients browse available CityMD locations and select which location they would like to book an appointment at. *See* Figure 1.

[38] *Id.* (emphasis added).

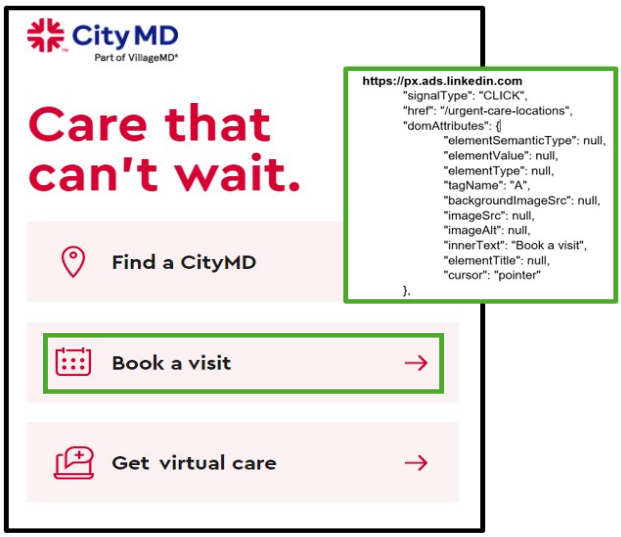

Figure 1: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

52. Unbeknownst to consumers, LinkedIn was tracking their activity the moment they entered the CityMD Website.

53. For example, the LinkedIn Insight Tag was embedded on the Website, which allowed LinkedIn to intercept and record "click" events. Click events detail information about which page on the Website the patient was viewing as well as the selections they were making. LinkedIn intercepts information including the patient's appointment time, who the appointment was for, why they were booking the appointment, and their gender. *See* Figures 1–5.

Figure 2: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

Figure 3: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

Figure 4: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

Figure 5: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

54. Through the LinkedIn Insight Tag, Defendant assisted LinkedIn in intercepting its patients' confidential information related to their medical appointments. Both Defendant and LinkedIn monetized this data for targeted advertising purposes.

55. As shown in Figures 2 through 5, Defendant assisted LinkedIn in intercepting several pieces of confidential information, including the location and time of a patient's appointment, their gender, and the type of medical appointment they were seeking treatment for.

56. These interceptions also included the li_sugr and lms_ads cookies, which LinkedIn utilizes to identify its account holders for targeted advertising.

57. LinkedIn incorporated the information it intercepted from the CityMD Website into its marketing tools to fuel its targeted advertising service.

58. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant or LinkedIn to intercept her confidential health information.

59. By law, Plaintiff is entitled to privacy in her protected health information and confidential communications. Defendant deprived Plaintiff of her privacy rights when it implemented a system that surreptitiously tracked and recorded Plaintiff's and other patients' confidential communications, personally identifiable information, and protected health information.

CLASS ACTION ALLEGATIONS

60. Plaintiff brings this action as a class action under Federal Rule of Civil Procedure 23 on behalf of all LinkedIn account holders in the United States who booked a medical appointment on www.citymd.com (the "Class").

61. Excluded from the Class is Defendant, the officers and directors of the Defendant at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which either Defendant has or had a controlling interest.

62. Plaintiff is a member of the Class she seeks to represent.

63. The Class is so numerous that joinder of all members is impractical. Although Plaintiff does not yet know the exact size of the Class, upon information and belief, the Class includes at least thousands of members.

64. The Class is ascertainable because the Class members can be identified by objective criteria – all LinkedIn account holders who booked an appointment on www.citymd.com. Individual notice can be provided to Class members "who can be identified through reasonable effort." Fed. R. Civ. P. 23(c)(2)(B).

65. There are numerous questions of law and fact common to the Class, which predominate over any individual actions or issues, including but not limited to:

A. Whether Defendant gave the Class members a reasonable expectation of privacy that their information was not being shared with third parties;

B. Whether Defendant's disclosure of information constitutes a violation of the claims asserted;

C. Whether Plaintiff and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

D. Whether Plaintiff and Class members have sustained damages as a result of Defendant's conduct and if so, what is the appropriate measure of damages or restitution.

66. Plaintiff's claims are typical of the claims of the members of the Class, as all members are similarly affected by Defendant's wrongful conduct. Plaintiff has no interests antagonistic to the interests of the other members of the Class. Plaintiff and all members of the Class have sustained economic injury arising out of Defendant's violations of common and statutory law as alleged herein.

67. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained counsel competent and experienced in prosecuting class actions, and she intends to prosecute this action

vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and her counsel.

68. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims are consistently adjudicated.

69. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

COUNT I
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1), *et seq.*

70. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

71. Plaintiff brings this Count individually and on behalf of the proposed Class.

72. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

73. The ECPA protects both sending and the receipt of communications.

74. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

75. The transmission of Plaintiff's PII and PHI to Defendant's Website qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

76. The transmission of PII and PHI between Plaintiff and Class members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

77. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

78. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

79. The ECPA defines "electronic, mechanical, or other device," as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5).

80. The following instruments constitute "devices" within the meaning of the ECPA:

(a) The computer codes and programs LinkedIn used to track Plaintiff and Class members communications while they were navigating the Website;

(b) Plaintiff's and Class members' browsers;

(c) Plaintiff's and Class members' mobile devices;

(d) Defendant and LinkedIn's web and ad servers;

(e) The plan Defendant and LinkedIn carried out to effectuate the tracking and interception of Plaintiff's and Class members' communications while they were using a web browser to navigate the Website.

81. Plaintiff and Class members' interactions with Defendant's Website are electronic communications under the ECPA.

82. By utilizing and embedding the LinkedIn Insight Tag on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class members in violation of 18 U.S.C. § 2511(1)(a).

83. Specifically, Defendant intercepted Plaintiff's and Class members' electronic communications through the LinkedIn Insight Tag, which tracked, stored and unlawfully disclosed Plaintiff's and Class members' PII and PHI to third parties, such as LinkedIn.

84. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class members regarding PII and PHI, including their LinkedIn account and treatment information. This confidential information was then monetized for targeted advertising purposes.

85. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class members' electronic communications to affiliates and other third parties, while knowing or

having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

86. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

87. Defendant intentionally intercepted the contents of Plaintiff's and Class members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy, among others.

88. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information ("IIHI") to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[39]

[39] 42 U.S.C. § 1320d-6.

89. Plaintiff's information that Defendant disclosed to LinkedIn qualifies as IIHI, and Defendant violated Plaintiff's and Class members' expectations of privacy. Such conduct constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6. Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the LinkedIn Insight Tag to track and utilize Plaintiff's and Class members' PII and PHI for financial gain.

90. Defendant was not acting under the color of law to intercept Plaintiff's and Class members' wire or electronic communications.

91. Plaintiff and Class members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class members' privacy through the LinkedIn Insight Tag. Plaintiff and Class members, all of whom are patients of Defendant, had a reasonable expectation that Defendant would not redirect their communications to LinkedIn without their knowledge or consent.

92. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq.*

93. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiff seeks statutory damages of the greater of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, *et seq.* under 18 U.S.C. § 2520.

COUNT II
BREACH OF FIDUCIARY DUTY/CONFIDENTIALITY

94. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

95. Plaintiff brings this Count individually and on behalf of the proposed Class.

96. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information. This duty arises from the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

97. Plaintiff and Class members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

98. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff's and Class members' PII and PHI, Defendant became a fiduciary by its undertaking and guardianship of this protected information, to act primarily for the benefit of its patients, including Plaintiff and Class members: (1) for the safeguarding of Plaintiff's and Class members' PII and PHI; (2) to timely notify Plaintiff and Class members of disclosure of their PII and PHI to unauthorized third parties; and (3) to maintain complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

99. Contrary to its duties as a medical provider and its implied promises of confidentiality, Defendant installed the LinkedIn Insight Tag to disclose and transmit to third parties Plaintiff's and Class members' communications with Defendant, including PII and PHI and the contents of such information.

100. These disclosures were made for commercial purposes without Plaintiff's or Class members' knowledge, consent, or authorization, and were unprivileged.

101. The unauthorized disclosures of Plaintiff's and Class members' PII and PHI were intentionally caused by Defendant's employees acting within the scope of their employment.

Alternatively, the disclosures of Plaintiffs' and Class members' PII and PHI occurred because of Defendant's negligent hiring or supervision of its employees, its failure to establish adequate policies and procedures to safeguard the confidentiality of patient information, or its failure to train its employees to properly discharge their duties under those policies and procedures.

102. The third-party recipients include LinkedIn. Such information was received by these third parties in a manner that allowed them to identify the Plaintiff and the individual Class members.

103. Defendant's breach of the common law implied covenant of trust and confidence is evidenced by its failure to comply with federal and state privacy regulations, including:

a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

b. By failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

c. By failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);

d. By failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiffs' and Class Members PHI;

e. By failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to

those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. By failing to implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);

g. By impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;

h. By failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);

i. By failing to keep PII and PHI confidential as required by N.Y. C.P.L.R. 4504;

j. By failing to keep PII and PHI confidential as required by N.Y. Pub. Health Law § 2803(3)(f); and

k. By otherwise failing to safeguard Plaintiff's and Class members' PII and PHI.

104. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

105. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;

b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. General damages for invasion of their rights in an amount to be determined by a jury;

e. Nominal damages for each independent violation;

f. Defendant took something of value from Plaintiff and Class members and derived benefit therefrom without Plaintiff's and Class members' knowledge or informed consent and without compensation for such data;

g. Plaintiff and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

h. Defendant's actions diminished the value of Plaintiff's and Class members' PII and PHI; and

i. Defendant's actions violated the property rights Plaintiff and Class members have in their PII and PHI.

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

a. Determining that this action is a proper class action;

b. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Class and naming Plaintiff's attorneys as Class Counsel to represent the Class;

c. For an order declaring that Defendant's conduct violates the statutes referenced herein;

d. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

e. Award compensatory damages, including statutory damages where available, to Plaintiff and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;

f. Ordering Defendant to disgorge revenues and profits wrongfully obtained;

g. For prejudgment interest on all amounts awarded;

h. For injunctive relief ordering Defendant to immediately cease its illegal conduct;

i. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit; and

j. Grant Plaintiff and the Class members such further relief as the Court deems appropriate.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all claims so triable in this action.

Dated: October 31, 2024

Respectfully submitted,

By: */s/ Alec Leslie*___

BURSOR & FISHER, P.A.
Alec M. Leslie
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: aleslie@bursor.com

BURSOR & FISHER, P.A.
Sarah N. Westcot (*pro hac vice* forthcoming)
Stephen A. Beck (*pro hac vice* forthcoming)
701 Brickell Ave., Suite 2100
Miami, FL 33131
Tel: (305) 330-5512
Fax: (305) 676-9006
E-Mail: swestcot@bursor.com
sbeck@bursor.com

Attorneys for Plaintiff